変える力を、ともに生み出す。
NTT DATAグループ

バックオフィス連携実験における ID連携技術の適用

平成22年12月14日

株式会社NTTデータ
リージョナルビジネス事業本部

INDEX

1　バックオフィス連携とは

1－1　総務省様　地域情報プラットフォーム推進事業とは
1－2　バックオフィス連携とは
1－3　バックオフィス連携において考慮すべき事項
1－4　現行イメージ
1－5　バックオフィス連携基盤　利用イメージ
1－6　バックオフィス連携により可能になる業務改革のパターン
1－7　バックオフィス連携基盤　システムイメージ
1－8　バックオフィス連携の要件と採用技術

2　バックオフィス連携における技術解説

2－1　バックオフィス連携に採用する技術
　① ID連携技術　SAML 2.0
　② プライバシ情報流通技術　ID-WSF 2.0
2－2　バックオフィス連携イメージ
2－3　具体的なユースケース
　① 職員による住民情報の自治体間連携
　② 住民情報を持つ自治体へのルーティング
　③ 住民本人の同意、許諾に基づく流通のコントロール

3　各施策の動向

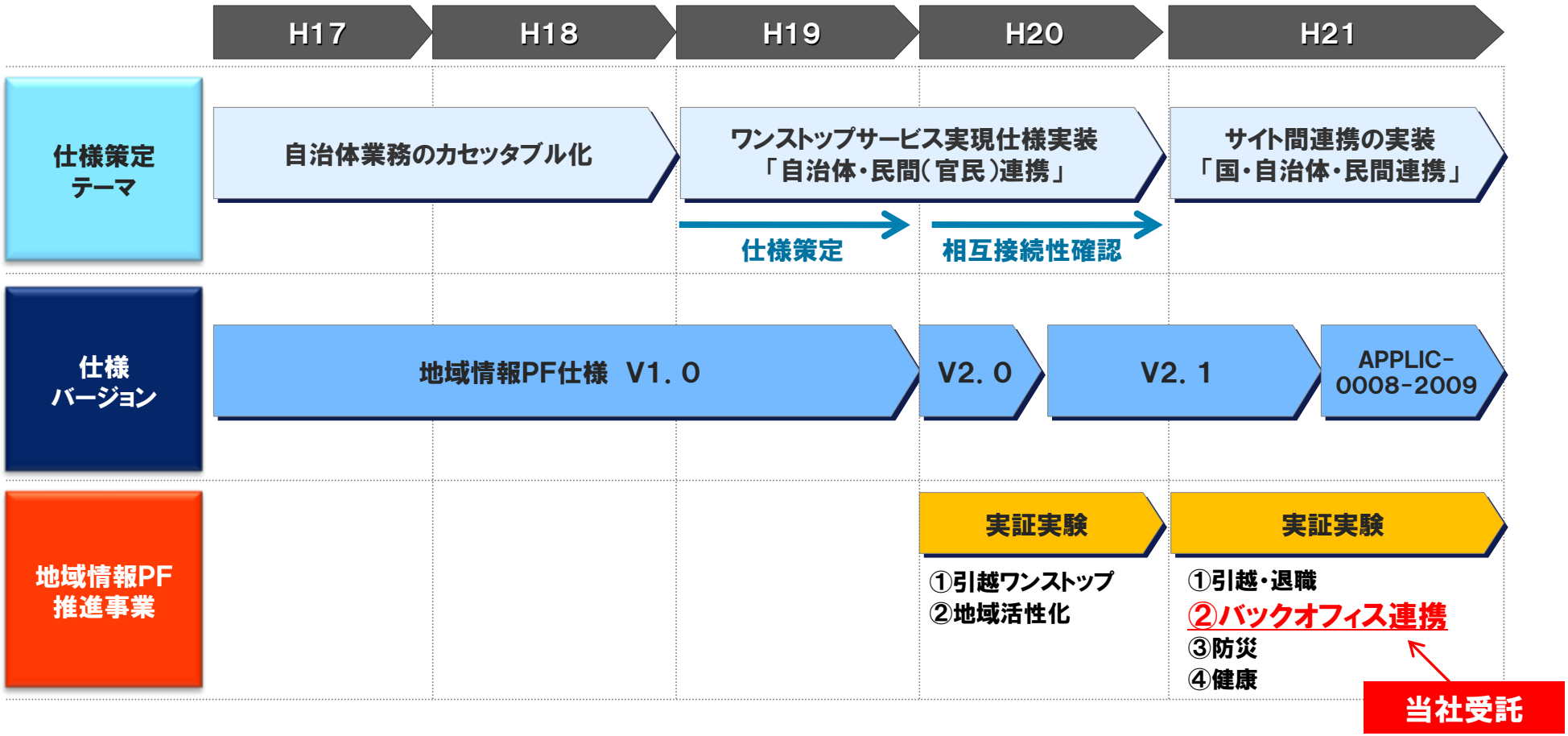
3－1　国の施策動向
3－2　ID-WSFに関する実証実験取り組み状況

1．バックオフィス連携とは

1－1．総務省様　地域情報プラットフォーム推進事業とは

変える力を、ともに生み出す。
NTT DATAグループ

・様々なシステム間の連携を可能にするための**標準仕様である地域情報プラットフォームを活用**する。
・地方公共団体間等における効率的な**業務システム連携**と最適な業務プロセスに向けた**業務改革**を行うことにより、**住民の利便性向上と行政の効率化を実現**する。
・その実現のために必要な検討・実証を行う。成果物は広く地方公共団体等に周知・提供する。

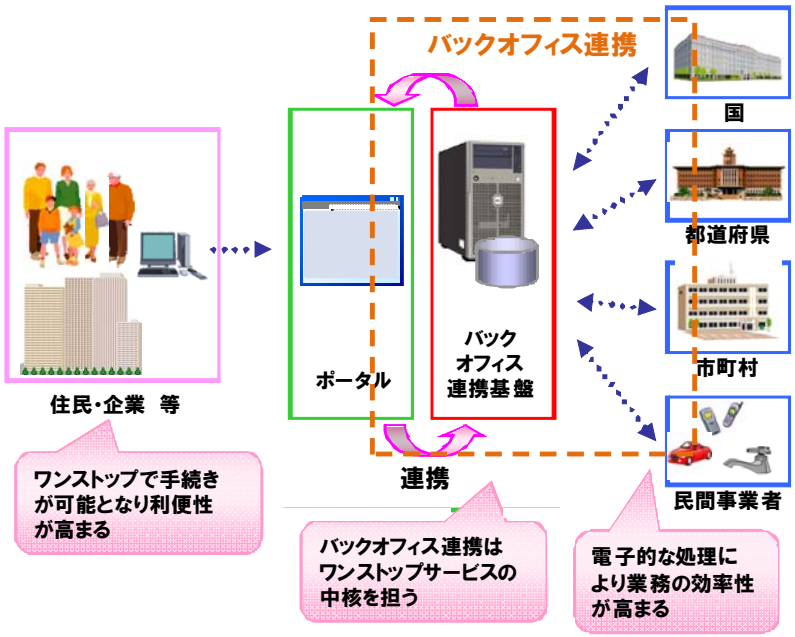


1－2．バックオフィス連携とは

バックオフィス連携は、情報を所有している各組織（情報保有機関）が相互に連携することにより情報を有効活用するものである。

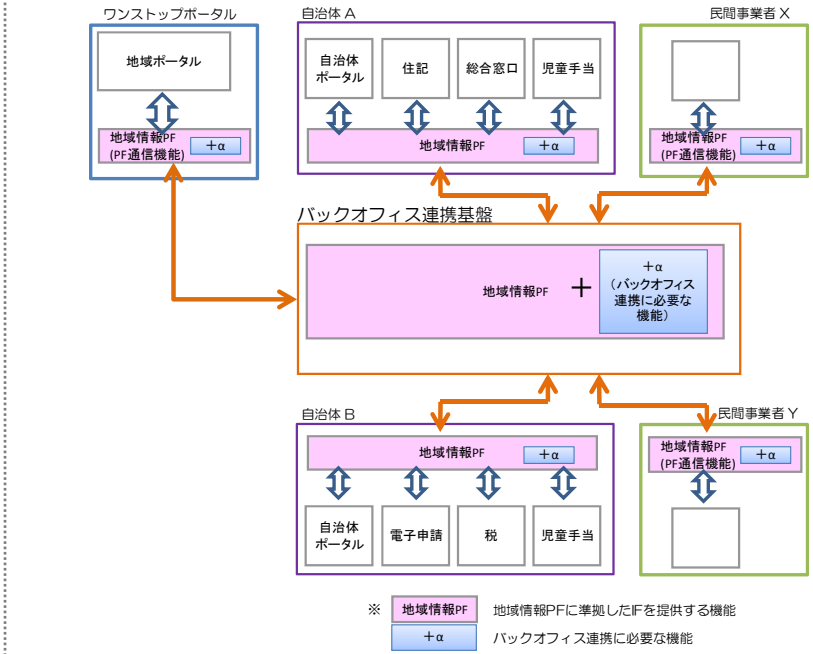
■ バックオフィス連携の目的

これまで電子行政の実現にあたっては、申請受付のオンライン化等フロントシステムに重点を置いてきたが、更なる電子行政の推進に向け、各情報保有機関同士が相互に連携する仕組みをつくる



■ バックオフィス連携基盤の役割

バックオフィス連携は地域情報PF標準仕様に準拠した標準仕様により実現する。実現にあたって各サイトにて共通的に利用する機能や情報の提供を行う



1－3. バックオフィス連携において考慮すべき事項

～住民の安心安全確保の重要性～

バックオフィス連携では様々な分野の機関・組織が連携することによって、多くの情報が流通する。
安心安全な情報流通や効率化を実現するため、以下の2つの観点で情報管理の最適化を行う。

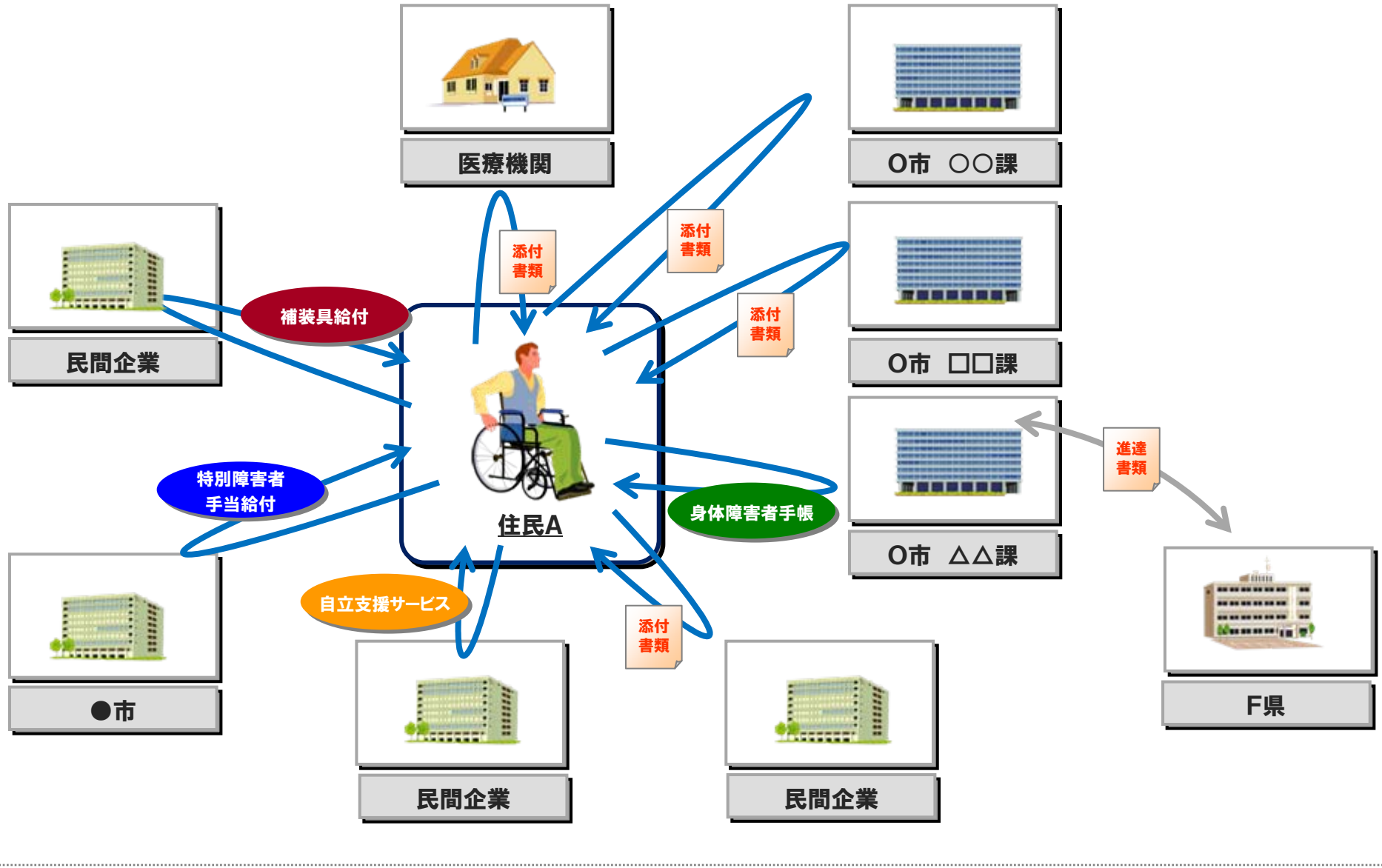
■ 安心・安全な情報の流通

- 住民自身によって、自らのプライバシ情報の流通などを指定できる
- 住民自身が、自らのプライバシ情報の行き先などを確認できる
- 国、県や市町村におけるプライバシ情報の管理と流通制御の責任主体を明確化する
- 国、県や市町村、民間事業者は、個々の住民により認可されたプライバシ情報利用の権限に基づき、プライバシ情報の提供と利用を行う
- 流通させるプライバシ情報を必要最低限の項目に絞りこむことにより、プライバシ情報の目的外利用の防止や、漏洩に対するリスク低減を図る

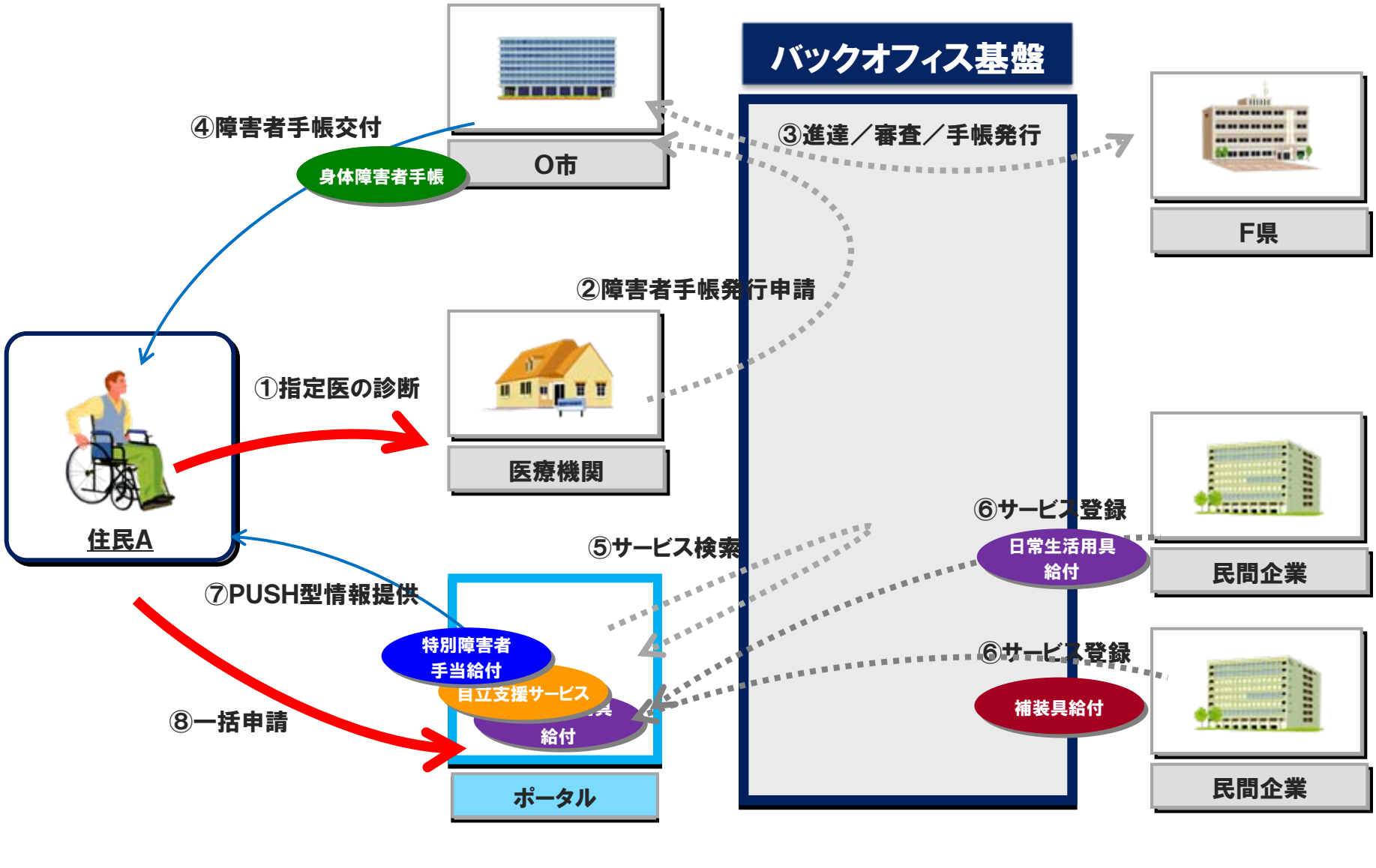
■ 情報管理の最適化

- プライバシ情報や権限等が、一極集中管理の基盤ではなく、それぞれの責任範囲に応じて分散管理する

1－4. 現行イメージ



1－5. バックオフィス連携基盤　利用イメージ



1－6. バックオフィス連携により可能になる業務改革のパターン
（障がい者福祉分野）

変える力を、ともに生み出す。
NTT DATAグループ

1 障がい者が**複数の手続を一括して申請**することを可能にする。

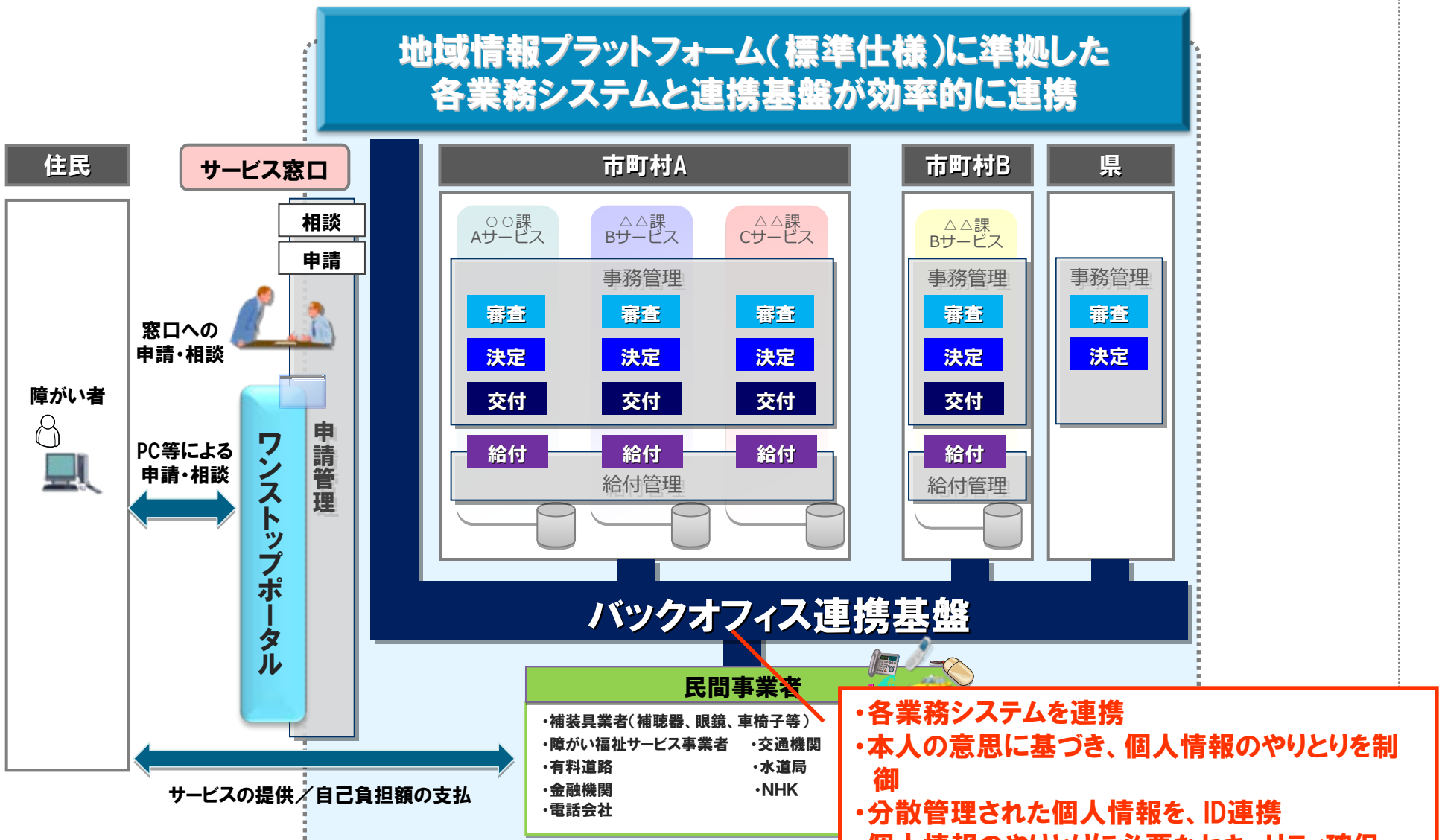
2 行政が保有している情報をもとに、行政側から、その障がい者が利用可能なサービス等を案内する（**プッシュ型のサービス案内**）。

3 申請、審査等に必要な情報は、**本人の同意を前提**に、行政が保有している情報を活用することで、**添付書類・手続や重複する作業を省略**することを可能にする。

4 市町村と県が**二段階で審査**している手続（例：身体障害者手帳の交付）について、市町村の形式審査を業務システムが行うことで効率化するとともに、市町村・県間のやりとりを電子的に行うこと等で手帳等を**早期に交付**する。

5 市町村において、サービスの種類にかかわらず給付状況を**一元的に管理**し、各事業者への支払いをまとめて行う。

1－7. バックオフィス連携基盤　システムイメージ



1－8. バックオフィス連携の要件と採用技術

生活者視点によるサービス提供、安心・安全なプライバシ情報の流通、および情報管理の最適化にあたって、バックオフィス連携に求めるべき要件と、バックオフィス連携を実現させる採用技術を以下に示す。

	要件	採用技術（策定団体）	説明
1	ワンストップサービスの提供	ビジネスプロセス管理技術： WS-BPEL2.0	複数の組織が相互に連携するため、手続きの実行順序や連携する各組織における処理状態を管理し情報の整合性を確保する。
2	情報の流通制御	プライバシ情報流通技術： ID-WSF2.0	プライバシ情報は一極集中管理されるのではなく、それぞれの責任範囲に応じて分散管理されている。ある機関がサービスを提供するために必要とする情報は、必要に応じて、原本を管理している情報保有機関から取得・利用する。
3	自己情報のコントロール	プライバシ情報流通技術： ID-WSF2.0	プライバシ情報流通にあたっては、情報所有者である本人によって情報流通先を指定できることが重要である。そのため本人自身によって自己情報の流通をコントロール（オプトイン／オプトアウト）する。 ただし、オプトアウトの要件を満たしている場合など、一定の条件に該当する場合は、本人の同意がなくとも第三者へ情報提供が可能である。
4	IDの紐付け	ID連携技術：SAML2.0	各保有機関で情報が分散管理されている状況では、各機関で保有する本人識別情報（ID）はそれぞれ異なる体系により管理されていることが想定される。 そのため、ID体系の異なる組織間での属性情報連携にあたっては、IDを紐づける。
5	情報流通先の把握	モニタリング技術／アクセス履歴	住民自身の情報が、誰に対して、どの範囲まで提供されているのかという、情報の所在やその流通先を可視化する。
6	プライバシ情報の安全性の確保	認証・認可・セキュリティ技術： SSL3.0/TLS1.0 XMLSignature XMLEncryption	バックオフィス連携は、外部ネットワークを介して情報を提供、取得、利用する仕組みである。ネットワークに流通する情報や各情報保有機関が保有する情報に対する様々な脅

バックオフィス連携実現にあたり、ID連携技術、プライバシ情報流通技術の選定の必要があった。

2. バックオフィス連携における技術解説

2－1．バックオフィス連携に採用する技術

バックオフィス連携の実現にあたり、ID連携技術、プライバシ情報流通技術の選定を行う必要があった。

要件

- バックオフィス連携を行う各機関が個別に技術を選定した場合、一部もしくはすべての情報連携ができなくなるなど制約が発生する可能性がある。
  （バックオフィス連携実現の標準技術の必要性）
- 自治体間の相互接続を図る場合、バックオフィス連携に必要な技術は地域情報プラットフォーム標準仕様にて標準化されることが必要である。
  （地域情報PF標準仕様に対する仕様補強の必要性）

課題

- ID連携やプライバシ情報流通に係るオープンな技術仕様は多数の団体により仕様策定されているが、デジュールやデファクトとして存在するものが少ない。

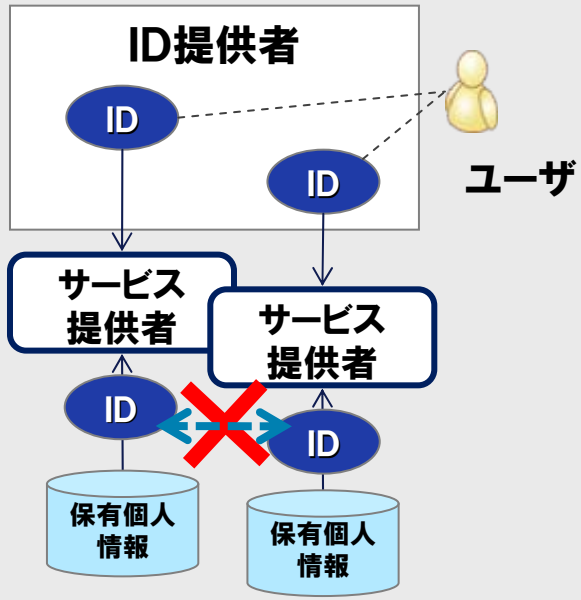
解決策

- ID連携技術やプライバシ情報流通技術をモデル化し、選定候補の技術仕様を分類する。
- バックオフィス連携のユースケースに即した評価項目を設定し、選定候補の技術仕様を評価する。
- 実証実験を通して、選定技術の有効性の確認する。

① ID連携技術　SAML 2.0

標準技術の選定にあたり、ID連携技術を以下の2パターンに整理した。

ID提供者中心モデル

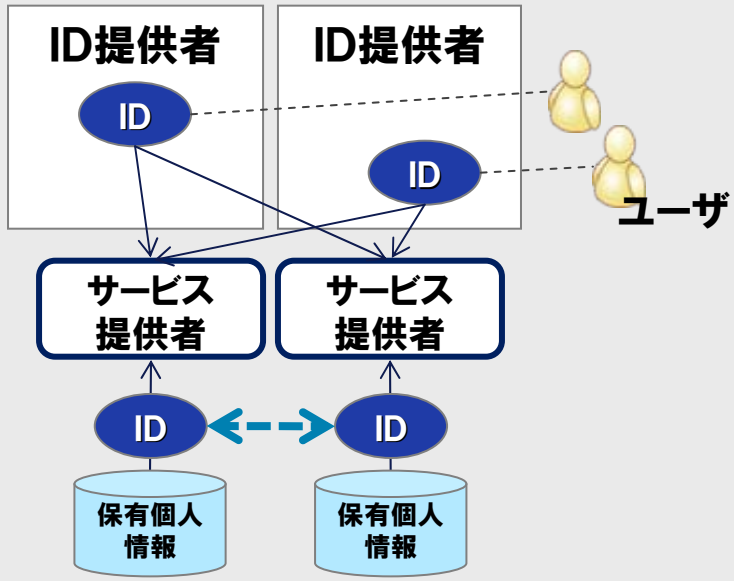


＜特徴＞
- ID提供者がID流通範囲を決定するモデル。
  - ID提供者とサービス提供者間で事前のトラストが必要
  - IDを公開する範囲はID提供者により制御される
- サービス提供者間で異なるID
  - サービス間でIDによる名寄せを防止できる
  - サービスごとのID変更運用が容易
- 単一のID提供者からサービス提供者にIDが供給される

＜実装技術＞
- SAML 2.0
- WS-Federation 1.1

閉域向け、高セキュリティ

ユーザ中心モデル



＜特徴＞
- ユーザがID流通範囲を決定するモデル
  - ID提供者とサービス提供者間で事前のトラストが不要
  - IDを公開する範囲はユーザが制御する
- サービス提供者間で同じID
  - サービス間でIDによる名寄せが容易
  - サービスごとのID変更運用が困難
- 複数のID提供者からサービス提供者にIDが供給されうる

＜実装技術＞
- OpenID 1.0/2.0
- CardSpace

広域向け、低セキュリティ

① ID連携技術　SAML 2.0

バックオフィス連携では、ID連携技術について、以下の要件が存在する。

- IDは、無制限に流通させるのではなく、自治体のみで流通させるなど流通範囲を制御できる必要がある。
- 自治体のIDで、他自治体の個人情報がマッチングできてはならない。
- 自治体ごとにIDを登録、抹消、変更などライフサイクル運用を行う必要がある。
- 自治体の保有個人情報とIDを紐付けるためには、厳格な本人確認のものにID発番を行う必要がある。
（発番主体となるID提供サイトは信頼がおける特定のサイトである必要がある。）

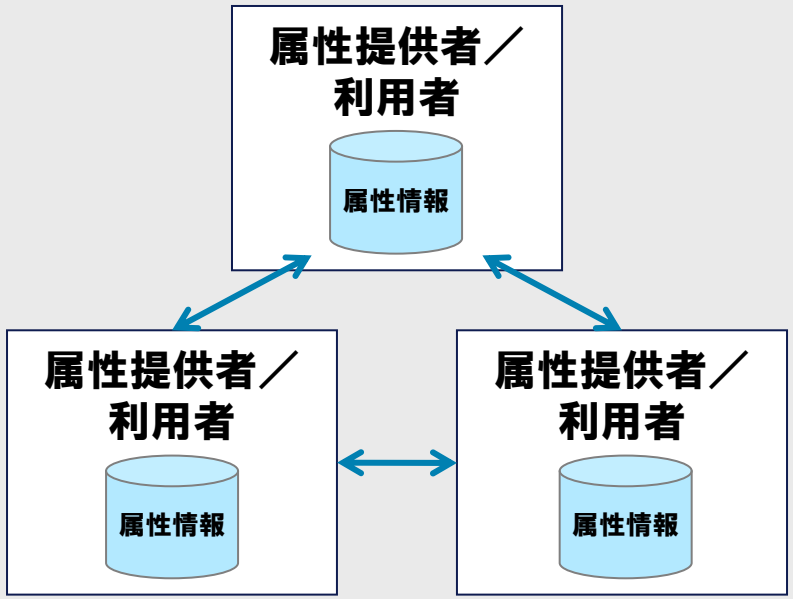
これら評価軸に基づき、様々な団体が仕様策定するID連携技術を評価し、SAML2.0の採用に至った。

	実験にて採用 SAML2.0	WS-＊	OpenID 1.0/2.0
ID連携モデル	ID提供者中心	ID提供者中心	ユーザ中心
事前トラスト	必要	必要	不要
仮ID（NameID）	対応	対応	非対応
ライフサイクル管理	対応	対応	非対応
ID提供者数	単一	単一	複数
実績	Force.com Google App Engine	実験段階	• Yahoo • mixi

② プライバシ情報流通技術　ID-WSF 2.0

標準技術の選定にあたり、プライバシ情報流通技術を以下の2パターンに整理した。

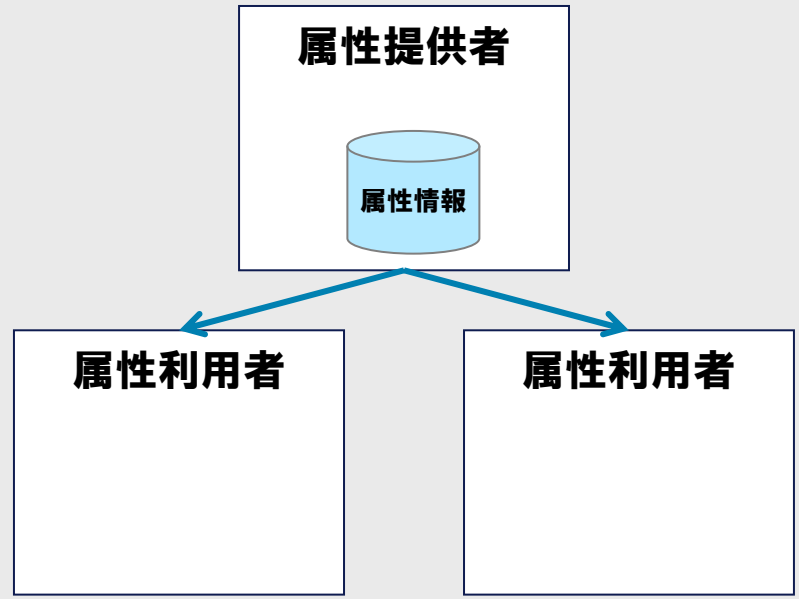
分散管理モデル



＜特徴＞
・属性情報が各サイトでそれぞれ管理される。
- サイトは、属性提供者および属性利用者両方の役割を担う。
- 必要な属性がどこにあるのかディスカバリが必要

＜実装技術＞
・ID-WSF 2.0
・WS-Federation 1.1

集約管理モデル



＜特徴＞
・属性情報が1つの中心的なサイトで管理される。
- サイトは、属性提供者と属性利用者に分類される。
- 必要な属性情報がどこにあるのかディスカバリは不要

＜実装技術＞
・OpenID AX 1.0
・OpenID SREG 1.0
・OAuth

② プライバシ情報流通技術　ID-WSF 2.0

バックオフィス連携では、プライバシ情報流通技術について、以下の要件が存在する。

- 自治体が既に保有している住民情報を連携するため、情報は各自治体に分散管理されている。
- 住民情報は、無制限に流通させるのではなく、自治体のみで流通させるなど流通範囲を制御できる必要がある。
- 職員が他自治体の住民情報を照会するなど、他ユーザの情報を連携させるケースが存在する。
- また、そういったケースでは、プライバシの観点から住民の許諾や同意に基づく流通制御が必要である。
- 分散管理モデルでは、情報所在の検索、サービスへのルーティングが必要となる。

これら評価軸に基づき、様々な団体が仕様策定するプライバシ情報流通技術を評価し、ID-WSF2.0の採用に至った。また、ID-WSF2.0はSAML2.0との仕様間の親和性が高く、最適な技術仕様と考えた。

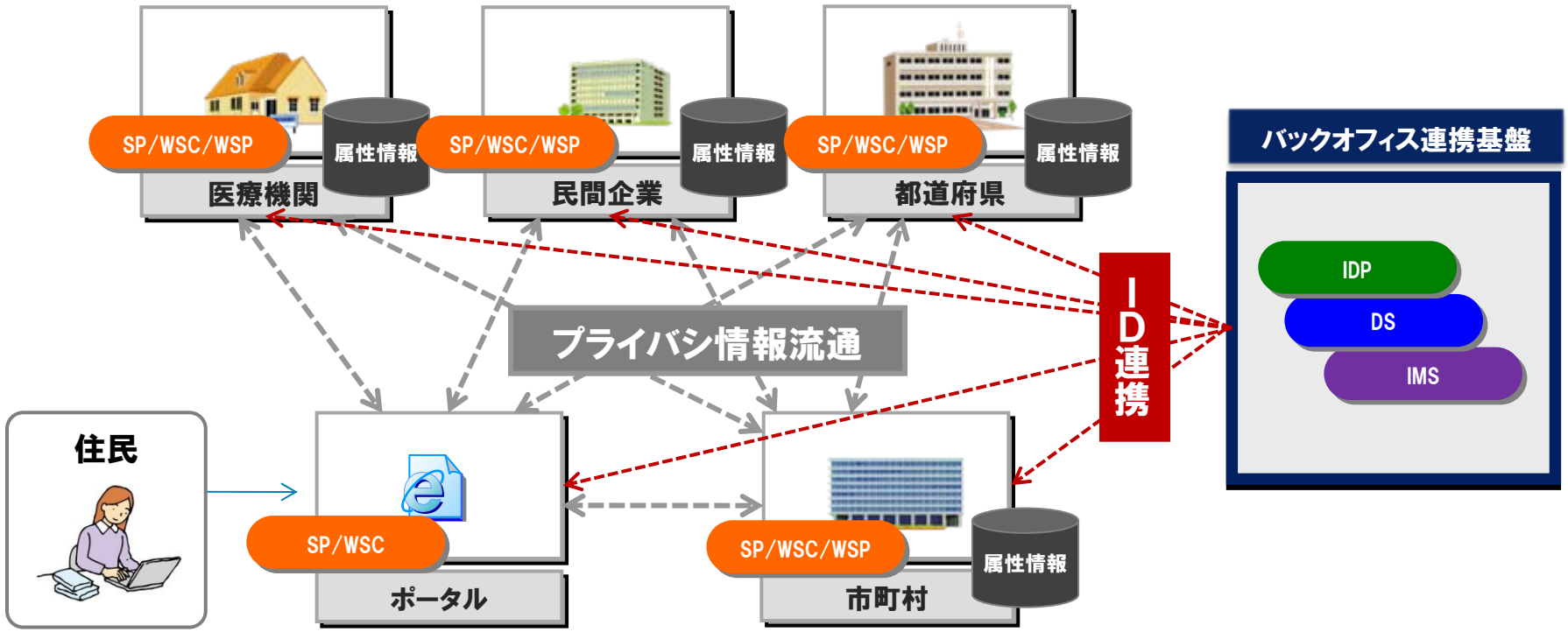
	実験にて採用 ID-WSF2.0	WS-＊	OpenID AX/SREG	OAuth
属性交換モデル	分散管理	分散管理	集約管理	集約管理
事前トラスト （流通範囲の制御）	必要	必要	不要	不要
他ユーザの情報連携	可能	不能	不能	不能
許諾に基づく流通 （流通制御）	可能	ー	ー	ー
属性ディスカバリ	可能	可能	ー	ー
実績	実験段階	実験段階	• Yahoo • mixi	• Twitter • Google

2－2. バックオフィス連携イメージ

技術仕様評価の結果を受け、バックオフィス連携実証では、以下の通り技術選定を行った。

- ID連携は、ID提供者中心モデル技術として、SAML2.0を採用。
- プライバシ情報流通は、分散管理モデル技術として、ID-WSF2.0を採用。

＜連携イメージ図＞



2－3. 具体的なユースケース

バックオフィス連携の具体的なユースケースとして、障がい者福祉分野を選定し、実証実験を行った。障がい者福祉分野では、県職員が市町村から障がい者情報を照会するなど団体間におけるプライバシ情報連携が必要であり、以下の問題が存在した。

以降では、これら問題をID連携技術、プライバシ情報連携技術を用い、どう解決したかについて解説する。

＜問題点＞

■ 住民のプライバシ情報を保有する自治体ロケーションの検索

・都道府県から、住民Aの情報を持つ市町村をどうやって発見するのか。

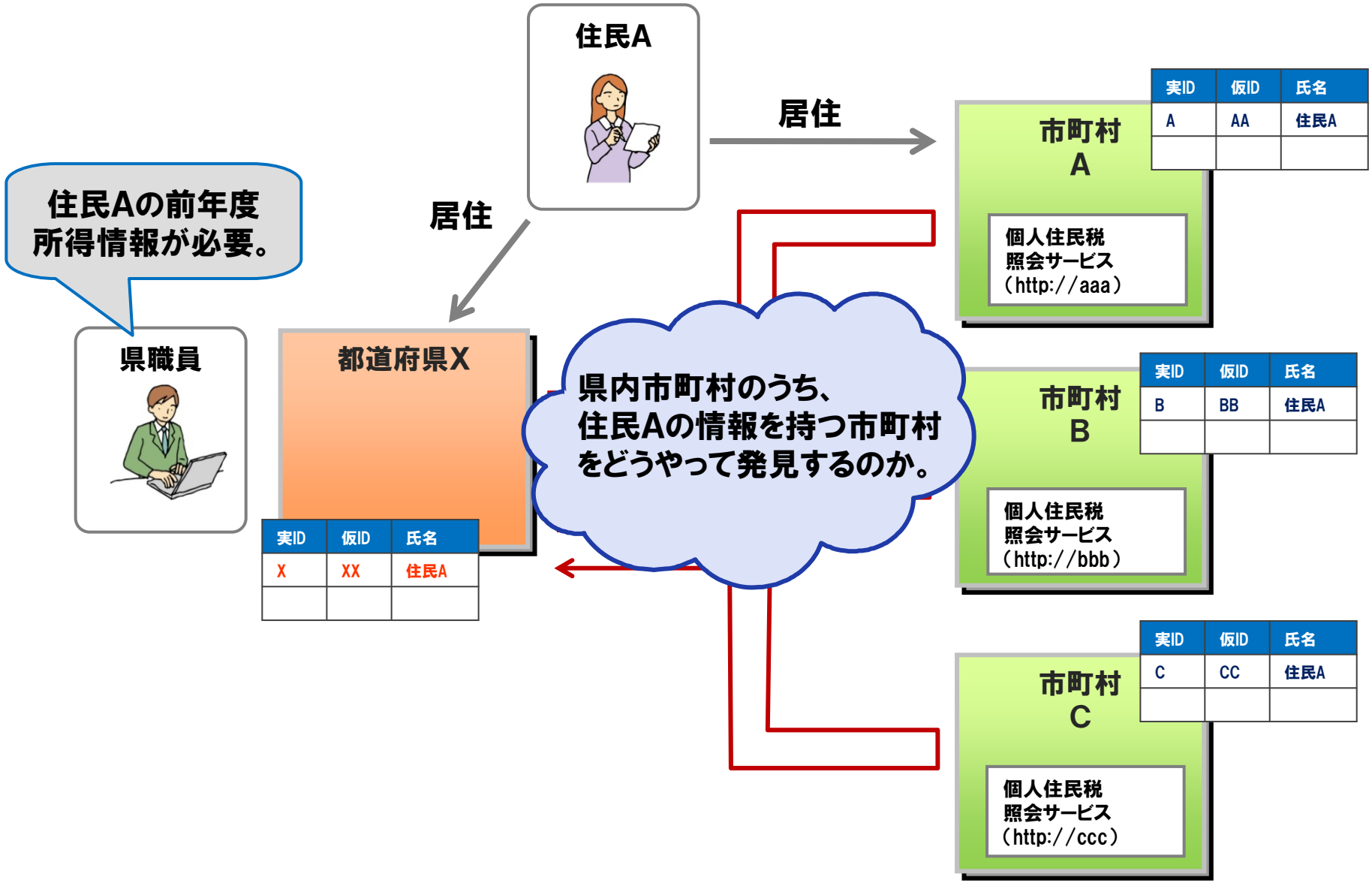
■ 職員認可に基づく住民のID変換

・都道府県と市町村で別IDで管理される住民をどう同定するのか。
・住民Aの情報を参照できる権限の範囲をどう限定するのか。

■ 住民の許諾、同意に基づくプライバシ情報の流通制御

・住民の許諾、同意に基づきどう情報連携をコントロールするか。
・住民の許諾、同意に基づき情報連携が行われていることをどう住民に知らせるか。

2－3. 具体的なユースケース
② 住民情報を持つ自治体へのルーティング



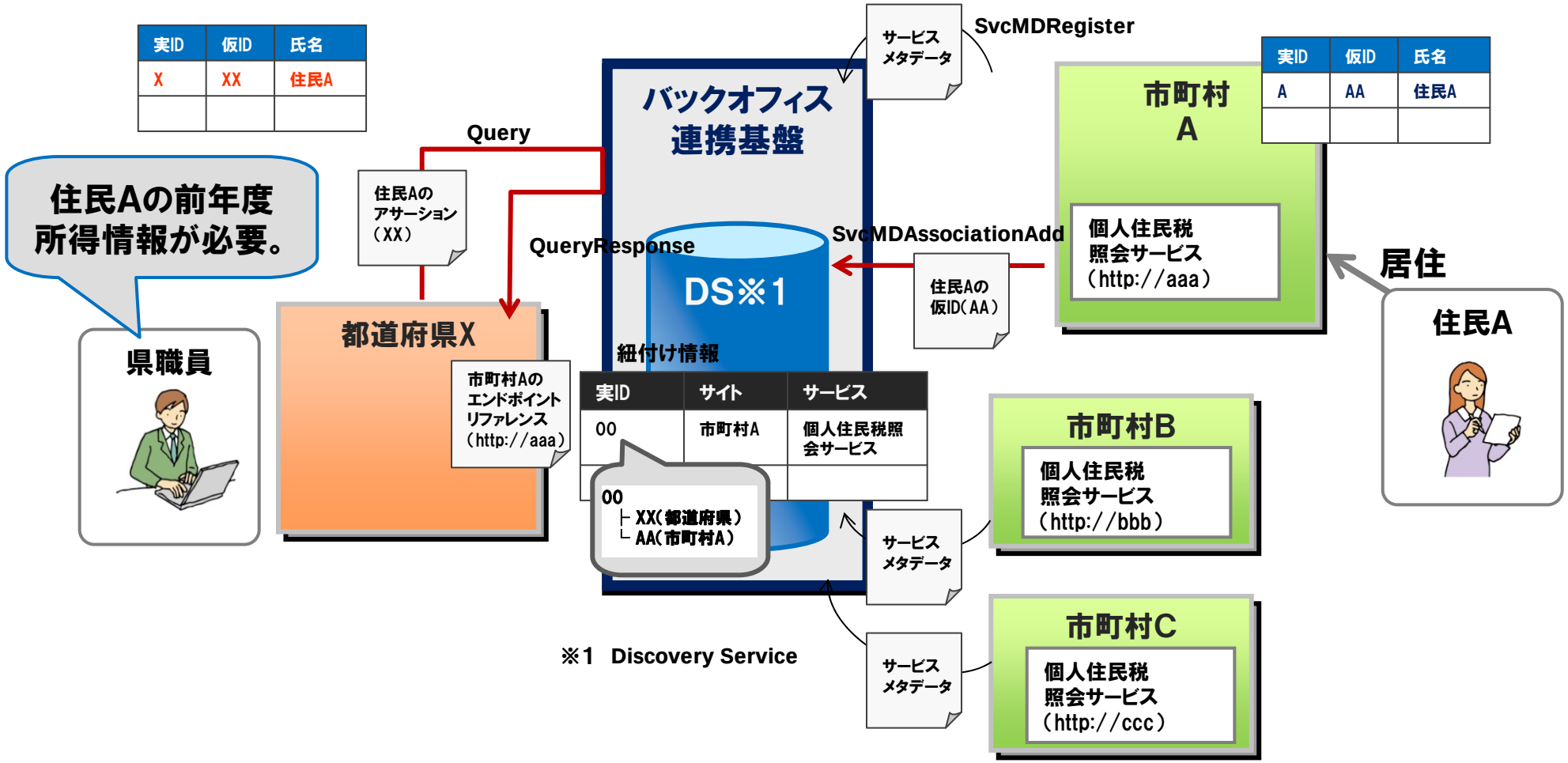
実ID	仮ID	氏名
X	XX	住民A

実ID	仮ID	氏名
A	AA	住民A

実ID	仮ID	氏名
B	BB	住民A

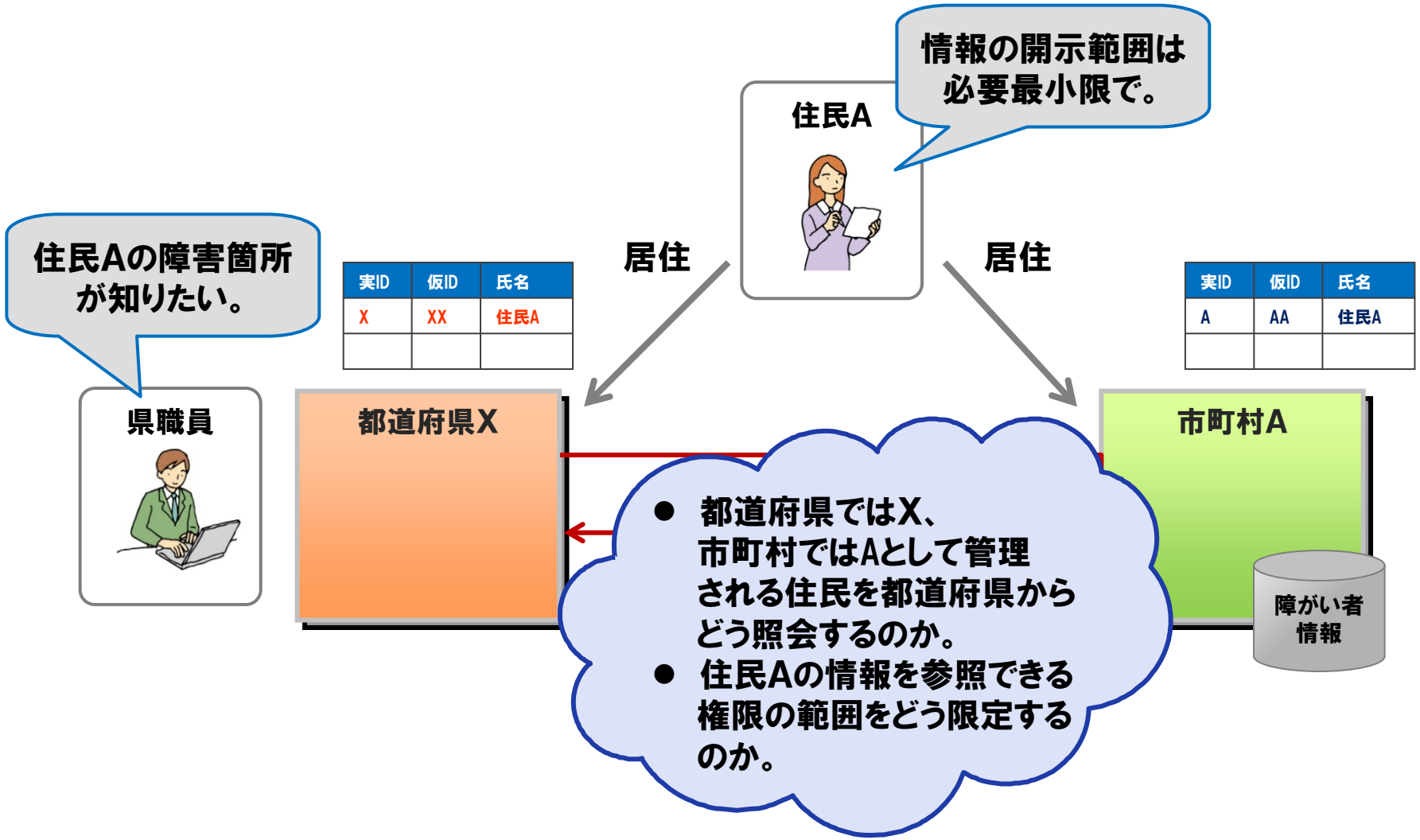
実ID	仮ID	氏名
C	CC	住民A

2－3. 具体的なユースケース
② 住民情報を持つ自治体へのルーティング

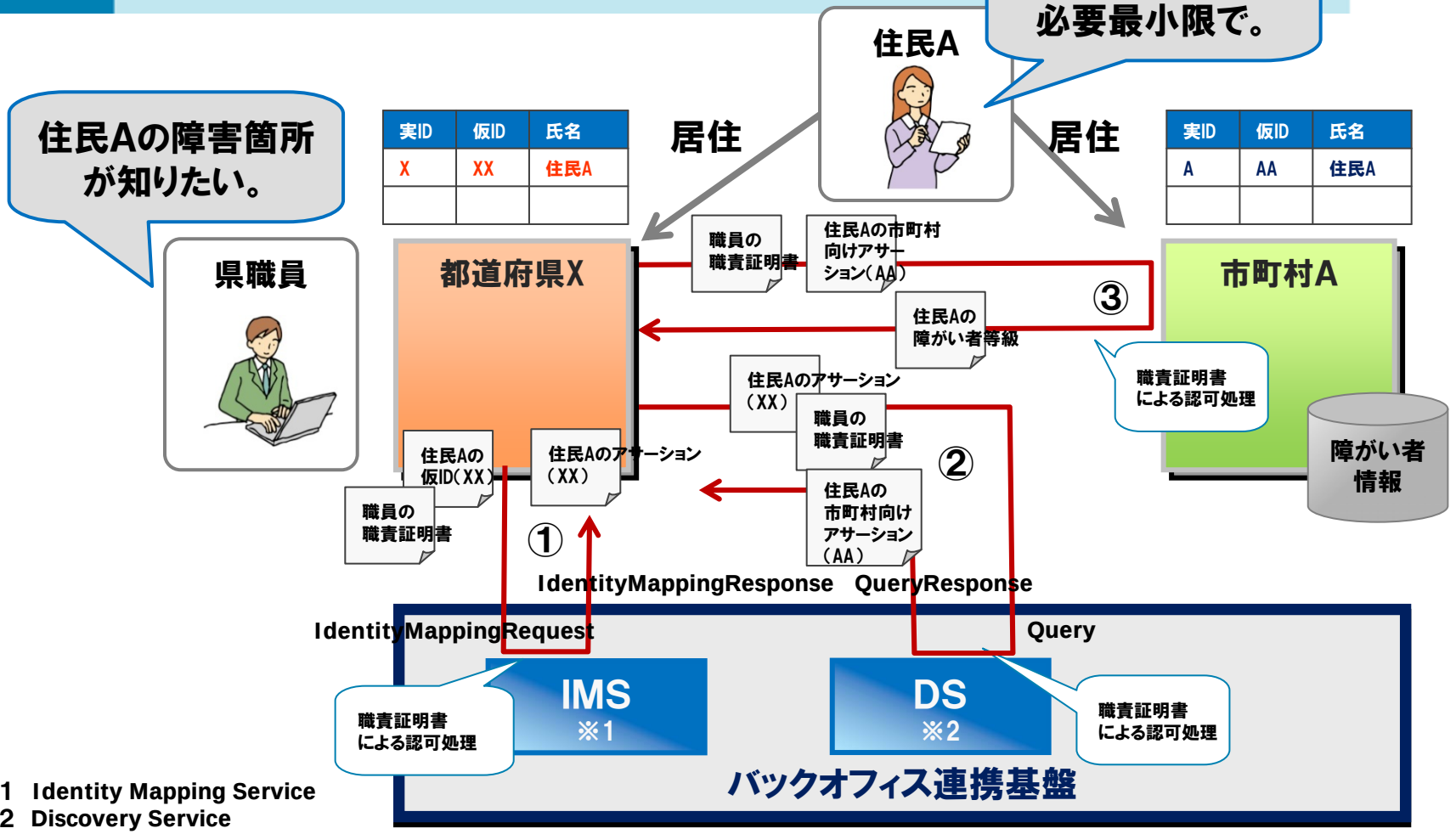


DSで、住民AのIDと市町村Aの個人住民税照会サービスの
紐づけ情報を管理し、都道府県にレジストリ情報を提供

① 職員認可に基づく住民のID変換



① 職員認可に基づく住民のID変換



※1 Identity Mapping Service
※2 Discovery Service

- **IMSとDSの組み合わせ**による住民Aの仮IDの変換
- **職責証明書（X.509 Token Profile）**による権限認可処理による他ユーザ情報連携権限の限定

③　住民本人の同意、許諾に基づく流通のコントロール

身体障害者手帳交付を受けたいけど、情報漏えいが心配。

申請

ポータル

- 住民の許諾、同意に基づきどう情報連携をコントロールするか。
- 住民の許諾、同意に基づき情報連携が行われていることをどう住民に知らせるか。

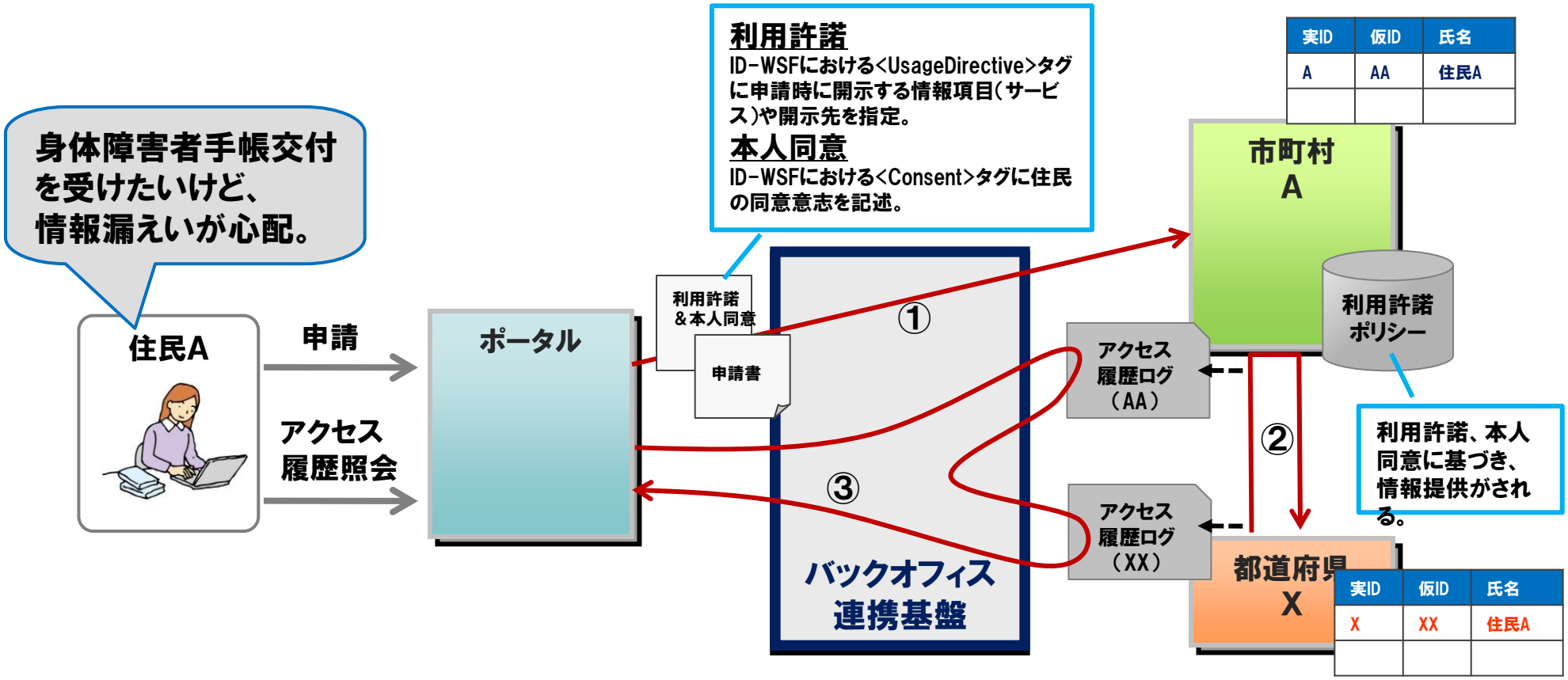
市町村
A

実ID	仮ID	氏名
A	AA	住民A

都道府県
X

実ID	仮ID	氏名
X	XX	住民A

③ 住民本人の同意、許諾に基づく流通のコントロール



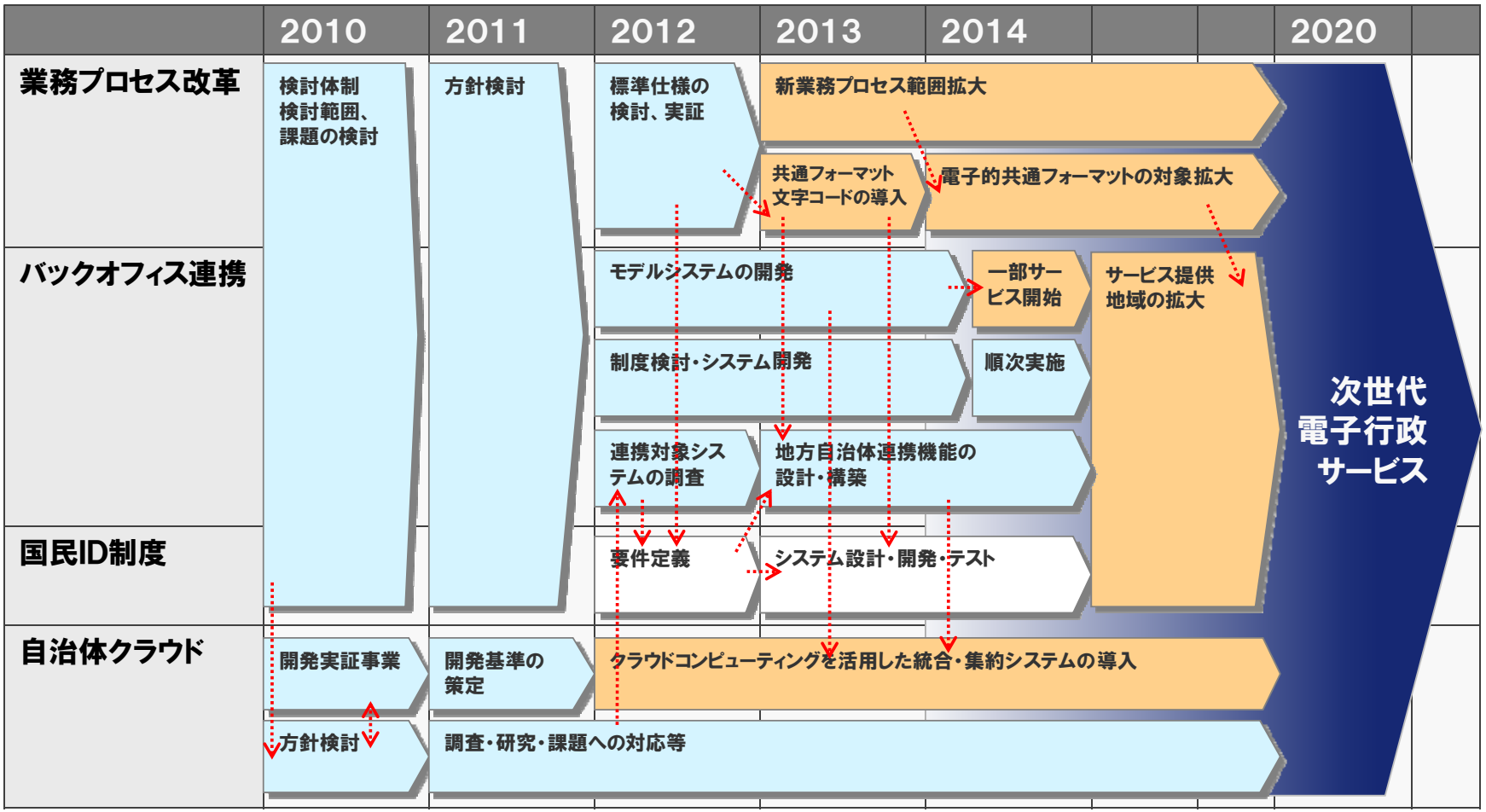
- 申請書に加えて**UsageDirective(利用許諾)、Consent(本人同意)**を連携させ流通制御に利用
- 自治体に分散出力される**アクセス履歴ログ**をバックオフィス連携基盤に**集約し、住民に開示**

3. 各施策の動向

3－1．国の施策動向

変える力を、ともに生み出す。
NTT DATAグループ

**バックオフィス連携は、H13．1月に内閣に設置されたIT戦略本部でも推進されており、
今後、関連の実証事業やタスクフォースでの議論が行われ、さらなる有効性の検証が行われる。
また、2020年を目標に50%の自治体で実サービス化が行われることが期待される。**



出典）IT戦略本部　新たな情報通信技術戦略 工程表

3－2. ID-WSFに関する実証実験取り組み状況

プライバシ情報流通技術は、複数団体により標準仕様化が進められているが、ID-WSFは、民間、国など様々な団体により実証実験が行われており、今後実サービス化が期待できる技術と言える。

■ Multi-Device SSOによるシームレスなコンテンツ視聴サービス（NHK）（2008年）

- http://wiki.projectliberty.org/images/a/a0/LADay_2008_03-02_Arisa_Fujii.pdf

■ 放送・通信融合サービスにおける認証連携の研究事例（NHK）（2010年）

- http://kantarainitiative.org/confluence/download/attachments/43876623/04_nhk_yamamura.pdf

■ 健康情報活用基盤　浦添市　（2009年）

・健康情報活用基盤（日本版EHR）の全体構想について）

- http://kantarainitiative.org/confluence/download/attachments/37749420/091106_ki_japan_conference_2009_05_yamamoto.pdf

・浦添地域健康情報活用基盤構築実証事業プロジェクト

- https://microsite.accenture.com/meti/Documents/201008/Accenture_METI_5_10.pdf

■ 社会保障カード実証事業　（2010年）

- http://www.mhlw.go.jp/stf/shingi/2r9852000000pbb9.html
- ・名張市社会保障カード（仮称）実証コンソーシアム発表資料（名張市）
- ・わかやま安心医療・社会保障カードコンソーシアム発表資料（海南市）
- ・いずも医療カード利用促進コンソーシアム発表資料（出雲市）
- ・かがわSSCコンソーシアム発表資料（高松市）
- ・福岡経済情報基盤コンソーシアム発表資料　（大野城市/前原市）
- ・おおむら社会保障カード（仮称）コンソーシアム発表資料（大村市）

■ 総務省　バックオフィス連携　（2009年）

- http://www.soumu.go.jp/main_content/000062031.pdf

■ 自治体クラウド開発実証に係る標準仕様書（2009年度）

- http://www.lasdec.nippon-net.ne.jp/cms/resources/content/17362/20100510-095726.pdf
- http://www.lasdec.nippon-net.ne.jp/cms/resources/content/17362/20100413-173624.pdf